

The Right to Privacy in the Era of Mass Surveillance in India: A Constitutional Perspective

Renu Rani

LLB, LLM, Kurukshetra University, Kurukshetra, Haryana, India

Received: 27 Jul 2024; Received in revised form: 23 Aug 2024; Accepted: 28 Aug 2024
©2024 The Author(s). Published by TheShillonga. This is an open-access article under the CC BY license
(<https://creativecommons.org/licenses/by/4.0/>)

Abstract

The expansion of digital technologies has significantly transformed state surveillance practices in India, raising complex constitutional questions concerning privacy, liberty, and democratic governance. This paper examines the right to privacy in the context of mass surveillance from a constitutional perspective. It analyses the evolution of privacy jurisprudence in India, culminating in its recognition as a fundamental right by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India. The study explores the nature and scope of mass surveillance, its impact on fundamental rights beyond privacy, and the limitations of the existing legal framework. It argues that unchecked surveillance poses risks to dignity, autonomy, and democratic participation. The paper concludes by emphasising the need for a rights-based surveillance framework grounded in constitutional principles, robust oversight, and accountability to ensure that security objectives do not erode fundamental freedoms.

Keywords— Fundamental Rights, Right to Privacy, Mass Surveillance, constitutional guarantees.

I. INTRODUCTION

The digital revolution has significantly changed the way modern states function. Everyday activities, such as communication, banking, travel, education, and accessing government services, increasingly depend on digital platforms. As a result, vast amounts of personal data are generated and stored in electronic form. This transformation has enabled governments to monitor, collect, and analyse information on a scale that was not possible in earlier times. Surveillance has thus shifted from limited observation of specific individuals to large-scale monitoring of populations through digital tools and networks.

Mass surveillance in the digital age typically involves the collection of communication data, internet activity, location information, and personal identifiers, often without the individuals' direct knowledge. Technologies such as data mining, artificial intelligence, and automated monitoring systems allow authorities to track patterns of behaviour rather than isolated acts. While such practices are commonly defended as necessary for national security, crime control, and public order, they raise serious concerns about the unchecked expansion of state power (Lyon, 2018). Continuous monitoring can blur the line between

lawful governance and intrusive control, especially when clear legal limits and safeguards are absent.

In democratic societies, surveillance is not inherently illegal; however, its scope and methods are crucial. Excessive or indiscriminate surveillance risks undermining trust between citizens and the state. When individuals believe they are constantly being watched, they may alter their behaviour, avoid expressing opinions freely, or withdraw from political participation. This makes mass surveillance not only a technological issue but also a social and constitutional one (Richards, 2013).

Privacy as a Constitutional Issue in India

In India, the importance of privacy as a constitutional concern has increased significantly with the expansion of digital governance. Government initiatives increasingly rely on databases, biometric identification, online platforms, and electronic records to deliver welfare schemes and public services. While these systems aim to improve efficiency and inclusion, they also create conditions for large-scale data collection and monitoring by the state. This raises important questions about how personal information is used, stored, and protected.

The constitutional importance of privacy was firmly established by the Supreme Court in Justice K.S.

Puttaswamy (Retd.) v. Union of India, where the Court recognised privacy as a fundamental right under Article 21 of the Constitution (Supreme Court of India, 2017). The judgment clarified that privacy is closely linked to human dignity, personal autonomy, and individual freedom. It also acknowledged that in a digital society, informational privacy—control over one's personal data—is especially important.

Mass surveillance directly challenges this constitutional understanding of privacy. Broad monitoring measures can interfere with personal choices, freedom of expression, and the right to dissent. Even when surveillance is carried out in the name of security, it must meet constitutional standards, including legality, necessity, and proportionality. Without these safeguards, surveillance practices risk becoming arbitrary and excessive (Bhatia, 2019). Moreover, surveillance not only affects privacy under Article 21 but can also indirectly restrict the freedoms guaranteed under Article 19, such as freedom of speech and association.

Therefore, privacy has become a central constitutional issue in contemporary India. It serves as a check on state power and a safeguard for democratic values. In the context of mass surveillance, examining privacy from a constitutional perspective is crucial to ensure that technological development enhances governance without compromising individual rights and civil liberties.

II. REVIEW OF LITERATURE

Bhandari (2020) examines how surveillance powers used for criminal investigation can conflict with constitutional rights following the Puttaswamy and Aadhaar judgments. The article argues that surveillance-related harms are not only about secrecy but also about power imbalance, profiling, and chilling effects. It emphasises stronger judicial review and oversight as constitutional necessities when the state deploys intrusive monitoring technologies.

Ramanathan (2010) critically evaluates India's unique identity project (UID/Aadhaar's early policy form) and warns that large identity databases can enable profiling, tracking, and surveillance. The review highlights how "efficiency" narratives can sideline constitutional concerns, such as consent, purpose limitation, and accountability. It is widely used in privacy scholarship to show how welfare-tech systems can expand state visibility into citizens' lives.

Objectives:

- i. To study the evolution of judicial interpretation of privacy in India.

- ii. To examine the constitutional limits on state surveillance powers.
- iii. To identify key challenges in regulating mass surveillance in India.

III. CONCEPTUAL FRAMEWORK OF THE RIGHT TO PRIVACY

The right to privacy is a multifaceted concept that protects individuals from unjustified intrusion by the state or other actors. At its core, privacy safeguards personal autonomy and human dignity by allowing individuals control over their bodies, personal information, and intimate decisions. Rather than being a single, narrow right, privacy operates as a cluster of related interests that together enable the free development of personality within a constitutional democracy (Westin, 1967).

Meaning and Dimensions of Privacy

Privacy is commonly understood through three interrelated dimensions: bodily, informational, and decisional privacy. Bodily privacy refers to the protection of an individual's physical integrity and autonomy. It limits forced bodily interventions such as intrusive searches, compulsory medical procedures, or biometric collection without lawful justification. This dimension emphasises that the human body is a private sphere deserving the highest degree of constitutional protection.

Informational privacy concerns the collection, storage, use, and dissemination of personal data. In the digital age, individuals generate vast amounts of data through routine activities, including communication, travel, and online transactions. Informational privacy recognises an individual's right to control how such data is accessed and processed, guarding against profiling, tracking, and misuse (Solove, 2010). It is this dimension that is most directly affected by mass surveillance practices.

Decisional privacy protects personal choices relating to intimate and fundamental aspects of life, including family relations, belief systems, and personal identity. This dimension ensures that individuals can make decisions free from coercion, monitoring, or fear of state interference. Together, these three dimensions form a comprehensive understanding of privacy as a condition necessary for liberty and self-determination.

Evolution of Privacy as a Legal Concept

The legal understanding of privacy has evolved gradually rather than emerging as an explicit right at once. Early constitutional jurisprudence in India did not clearly recognise privacy as a fundamental right, treating it as an implied or incidental interest. Over time, courts began to acknowledge that personal liberty would be incomplete

without some degree of privacy protection. This evolution culminated in Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court affirmed privacy as a constitutionally guaranteed right derived primarily from Article 21 and supported by Articles 14 and 19 (Supreme Court of India, 2017).

The judgment marked a shift from viewing privacy as a privilege to recognising it as a foundational constitutional value. It established that privacy is not absolute but can only be restricted through a law that satisfies tests of legality, necessity, and proportionality.

Privacy in the Context of Technological Advancement

Technological advancement has significantly altered the nature of privacy threats. Surveillance technologies enable continuous, automated, and large-scale monitoring, often without direct physical intrusion. Data aggregation and algorithmic analysis can reveal intimate details about individuals even when collected information appears harmless in isolation (Lyon, 2018). In this context, privacy serves as a constitutional check on technological power, ensuring that innovation and governance do not erode individual freedom. The conceptual framework of privacy thus provides the normative basis for evaluating surveillance practices in a digital constitutional order.

Constitutional Recognition of the Right to Privacy in India

The constitutional recognition of the right to privacy in India has been the result of a gradual and evolving judicial process rather than an explicit constitutional provision. The Indian Constitution does not expressly mention privacy as a fundamental right. Consequently, its status was initially uncertain and developed through judicial interpretation of existing fundamental rights, particularly those relating to liberty, equality, and freedom.

Early Judicial Approach: Pre-2017 Position

In the early years, Indian courts adopted a cautious and fragmented approach towards privacy. In *M.P. Sharma v. Satish Chandra* (1954), the Supreme Court rejected the argument that privacy was a guaranteed constitutional right, holding that the Constitution did not contain any explicit protection for it. Similarly, in *Kharak Singh v. State of Uttar Pradesh* (1963), the majority denied the existence of a fundamental right to privacy, although the minority opinion recognised privacy as an essential aspect of personal liberty. Despite this reluctance, later decisions gradually expanded the scope of Article 21, indirectly accommodating privacy-related concerns in cases involving personal liberty, dignity, and individual autonomy. However, until 2017, privacy remained an

implied and contested concept rather than a clearly defined constitutional right.

Privacy under Articles 14, 19, and 21

Over time, judicial interpretation has established that privacy draws constitutional protection from multiple provisions. Article 21, which guarantees the right to life and personal liberty, became the primary source for privacy protection. Courts interpreted “personal liberty” to include freedom from arbitrary state interference in private life. Article 14 reinforces privacy by requiring fairness, non-arbitrariness, and equality in state action, thereby limiting discretionary and discriminatory intrusions into personal space. Article 19 further strengthens privacy by safeguarding freedoms of speech, expression, movement, and association, all of which can be indirectly restricted through surveillance and excessive monitoring. Together, these articles establish a constitutional framework in which privacy serves as a fundamental condition for the meaningful enjoyment of basic rights.

Transformative Impact of Justice K.S. Puttaswamy (Retd.) v. Union of India

The constitutional status of privacy was conclusively settled in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). A unanimous nine-judge bench recognised privacy as a fundamental right inherent in human dignity and autonomy. The judgment marked a transformative shift by rejecting earlier precedents and establishing that any restriction on privacy must satisfy the tests of legality, necessity, and proportionality. This decision repositioned privacy as a foundational constitutional value, providing a robust framework for evaluating state actions, particularly in the context of surveillance and digital governance.

Doctrinal Foundations: Privacy, Dignity, and Autonomy

The constitutional doctrine of privacy is deeply intertwined with the concepts of human dignity and individual autonomy. Privacy is not merely a defensive right against state intrusion; it functions as a foundational value that enables individuals to live with self-respect, make meaningful choices, and participate freely in democratic life. Indian constitutional jurisprudence increasingly recognises privacy as a condition necessary for the realisation of dignity and autonomy rather than as an isolated or abstract entitlement.

Privacy as an Intrinsic Part of Human Dignity

Human dignity lies at the heart of the Indian Constitution and informs the interpretation of fundamental rights. Privacy is intrinsically linked to dignity because it protects the inner sphere of the individual from unwanted exposure, control, or humiliation. When the state intrudes into

personal spaces—whether physical, decisional, or informational—it risks reducing individuals to mere objects of governance. The Supreme Court has affirmed that dignity requires recognition of the individual as a moral agent capable of controlling personal aspects of life. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Court held that privacy preserves the “sanctity of the individual” and is essential for maintaining self-worth and personal integrity (Supreme Court of India, 2017). Thus, privacy is not only about secrecy but about respect for personhood.

Informational Self-Determination

Informational self-determination refers to the individual's ability to control the collection, use, and disclosure of personal data. This concept emerged prominently in comparative constitutional law and has gained renewed relevance in the digital age. Modern governance relies heavily on data-driven decision-making, making personal information a source of power. Without control over personal data, individuals may be subject to profiling, behavioural prediction, and social sorting. Informational self-determination ensures that individuals remain participants rather than passive subjects in digital systems (Solove, 2010). Indian constitutional thought now recognises that data protection and privacy safeguards are essential to prevent the misuse of personal information by both the state and private entities.

Individual Autonomy and Democratic Citizenship

Autonomy refers to an individual's capacity to make decisions about their life without coercion or constant monitoring. Privacy enables autonomy by creating spaces for free thought, expression, and association. In a democracy, citizens must be able to question authority, form opinions, and engage in dissent without fear of surveillance. Excessive monitoring can produce a chilling effect that undermines democratic participation (Richards, 2013). Therefore, privacy supports democratic citizenship by safeguarding individual freedom and pluralism. As a doctrinal principle, privacy serves as a constitutional shield, preserving the balance between state authority and individual self-governance in a democratic society.

Mass Surveillance in India: Nature and Scope

Mass surveillance refers to the systematic and large-scale monitoring of individuals or groups through the collection and analysis of data, often without specific suspicion against particular persons. Unlike conventional surveillance, which focuses on identified targets, mass surveillance operates by gathering information about entire populations or broad sections of society. Its defining characteristics include scale, continuity, automation, and secrecy. Such surveillance relies on the routine

interception of communications, metadata collection, location tracking, and database integration, raising serious concerns about transparency and accountability (Lyon, 2018).

In India, surveillance practices have gradually shifted from targeted monitoring to population-wide observation. Earlier surveillance mechanisms were primarily used for criminal investigation or national security purposes and required some degree of individual suspicion. However, with advances in technology and governance digitisation, surveillance now increasingly functions on a preventive and predictive logic. Data is collected first and analysed later to identify patterns, risks, or potential threats. This shift blurs the distinction between suspects and ordinary citizens, subjecting everyone to the possibility of monitoring (Richards, 2013). Such an approach significantly expands state power while weakening traditional safeguards like warrants and judicial oversight.

Digital technologies play a central role in enabling mass surveillance in India. The widespread use of mobile phones, internet platforms, biometric identification systems, and digital public services generates vast quantities of personal data. Data aggregation enables the combination and analysis of information from various sources, including identity databases, communication records, and service delivery platforms. Even data that appears harmless in isolation can reveal sensitive personal details when aggregated (Solove, 2010). Consequently, digital surveillance transforms personal information into a powerful tool of governance, making constitutional scrutiny essential to ensure that surveillance practices remain consistent with fundamental rights and democratic principles.

Legal Framework Governing Surveillance in India

India's surveillance regime is shaped by a mix of statutory provisions and executive rules rather than a single, comprehensive law. This structure has resulted in wide surveillance powers with limited external oversight, raising constitutional concerns in the post-privacy era.

1. Statutory Provisions Enabling Surveillance

- i. Surveillance powers in India arise from multiple sector-specific laws enacted for purposes such as national security, public order, and crime prevention.
- ii. These laws authorise interception of communications, access to stored data, and monitoring of digital activity when the state considers it necessary.
- iii. Key statutory terms like “public safety” and “sovereignty” are broadly framed, allowing

expansive interpretation by authorities (Bhandari, 2020).

- iv. The absence of a unified surveillance statute leads to fragmented regulation and weak transparency.

2. Surveillance Powers under the Information Technology Regime

- i. The Information Technology Act, 2000, provides the principal legal basis for digital surveillance in India.
- ii. It empowers the government to intercept, monitor, and decrypt information transmitted through computer resources.
- iii. These powers are operationalised through subordinate rules that specify authorisation procedures and internal review mechanisms.
- iv. Oversight under this regime is predominantly executive-driven, with little scope for prior judicial approval.
- v. Scholars argue that such internal checks are insufficient to meet constitutional standards of proportionality and accountability in digital surveillance (Solove, 2010).

3. Executive Discretion and Delegated Legislation

- i. A distinctive feature of India's surveillance framework is its reliance on delegated legislation, such as rules and executive orders.
- ii. Many procedural safeguards are contained in subordinate instruments rather than primary parliamentary statutes.
- iii. This limits democratic scrutiny and weakens institutional accountability.
- iv. Concentration of surveillance authority within the executive increases the risk of arbitrariness, particularly in the absence of independent oversight bodies.
- v. These concerns have become more pronounced after the recognition of privacy as a fundamental right, necessitating stronger legislative safeguards.

Constitutional Limits on State Surveillance

The exercise of surveillance powers by the state is not unrestricted under the Indian Constitution. After the recognition of privacy as a fundamental right, state surveillance must operate within clearly defined constitutional limits. These limits ensure that the pursuit of national security and public order does not undermine individual liberty, dignity, and democratic accountability.

Test of Legality, Necessity, and Proportionality

A central constitutional limitation on surveillance is the threefold test of legality, necessity, and proportionality, articulated by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India. Legality requires that any surveillance measure must be authorised by a valid law enacted through proper legislative procedure. Necessity demands that surveillance be justified by a legitimate state aim, such as national security or prevention of serious crime. Proportionality requires a rational connection between the objective and the means used, ensuring that the least intrusive method is adopted (Supreme Court of India, 2017). Indiscriminate or excessive data collection fails this constitutional standard.

Procedural Safeguards and Due Process Requirements

Procedural safeguards form an essential component of constitutional protection against misuse of surveillance powers. Due process requires clear rules governing authorisation, duration, scope, and review of surveillance measures. Individuals must be protected against arbitrary or secret monitoring through well-defined procedures and record-keeping requirements. The absence of transparent processes and independent review mechanisms increases the risk of abuse and undermines constitutional guarantees of fairness under Articles 14 and 21 (Bhandari, 2020).

Judicial Oversight and Accountability Mechanisms

Judicial oversight plays a crucial role in maintaining constitutional balance. Courts act as guardians of fundamental rights by reviewing the legality and proportionality of surveillance actions. Effective accountability mechanisms, including post-facto review, remedies for unlawful surveillance, and independent oversight bodies, are essential to prevent concentration of power within the executive. Without such checks, surveillance risks eroding trust in democratic institutions and weakening constitutional governance (Richards, 2013).

Judicial Responses to Surveillance Practices

Indian courts have played a significant role in shaping the constitutional boundaries of surveillance by interpreting statutory powers in light of fundamental rights. Judicial responses reflect a gradual shift from deference to executive authority toward rights-based scrutiny, particularly where surveillance interferes with personal liberty and privacy. Courts have consistently emphasised that surveillance laws must not be exercised arbitrarily and must conform to constitutional principles of fairness and reasonableness.

Interpretation of Surveillance Laws by Indian Courts

One of the earliest and most influential judicial interventions was in *People's Union for Civil Liberties v.*

Union of India, where the Supreme Court examined the constitutionality of telephone tapping. The Court acknowledged that interception of communications constitutes a serious invasion of privacy and therefore must be accompanied by procedural safeguards. It laid down detailed guidelines governing authorisation, duration, and review of interception orders, thereby reading due process requirements into surveillance laws (Supreme Court of India, 1997). This decision marked a departure from uncritical acceptance of executive surveillance powers.

Balancing National Security and Fundamental Rights

Indian courts have recognised that national security is a legitimate state interest, but have cautioned that it cannot override fundamental rights without a justifiable reason. In later jurisprudence, particularly following Justice K.S. Puttaswamy (Retd.) v. Union of India, courts have increasingly applied proportionality analysis to strike a balance between security concerns and individual freedoms. Judicial reasoning now stresses that security measures must be narrowly tailored and supported by law. This evolving approach reflects an effort to ensure that surveillance serves democratic governance rather than undermining constitutional liberties.

Mass Surveillance and Fundamental Rights Beyond Privacy

Mass surveillance affects not only the right to privacy but also several other fundamental rights guaranteed by the Indian Constitution. Continuous monitoring of communications and digital behaviour alters how individuals express themselves, participate in public life, and experience equality before the law. These broader constitutional implications make surveillance a systemic rights issue rather than a single-right concern.

Impact on Freedom of Speech and Expression

Freedom of speech and expression under Article 19(1)(a) depends on the ability of individuals to communicate ideas without fear of monitoring or reprisal. Mass surveillance can indirectly restrict this freedom by creating awareness or suspicion that communications are being tracked. Indian courts have recognised that state actions affecting online speech must be carefully scrutinised. In *Shreya Singhal v. Union of India*, the Supreme Court highlighted the importance of protecting free expression in digital spaces, noting that vague and overbroad restrictions can suppress legitimate speech (Supreme Court of India, 2015). Surveillance regimes that lack clear limits risk producing similar effects.

Chilling Effect on Dissent and Democratic Participation

A key democratic concern associated with mass surveillance is its chilling effect on dissent. When individuals believe their communications, associations, or movements are constantly observed, they may avoid expressing critical opinions or engaging in protests. This self-censorship weakens democratic participation and reduces the diversity of viewpoints essential to a constitutional democracy (Penney, 2017). Surveillance thus reshapes citizen behaviour, not through direct censorship but through psychological pressure.

Equality and Non-Discrimination Concerns

Mass surveillance also raises issues under Article 14 relating to equality and non-discrimination. Data-driven surveillance systems may disproportionately target specific communities based on profiling, location, or socio-economic characteristics. Algorithmic bias and selective enforcement can perpetuate existing social inequalities, resulting in unequal exposure to monitoring and state control (Eubanks, 2018). Without transparency and accountability, surveillance practices risk deepening structural discrimination, undermining the constitutional promise of equal protection under the law.

Comparative Constitutional Perspectives: At International Level

Comparative constitutional experience demonstrates that democratic states are increasingly regulating surveillance through robust, rights-based frameworks. In the European Union, courts have strictly limited mass surveillance by emphasising necessity and proportionality. In *Digital Rights Ireland Ltd v. Minister for Communications*, the Court of Justice of the European Union ruled that blanket data retention laws violated privacy and data protection rights, emphasising that indiscriminate collection is incompatible with democratic values (CJEU, 2014). Similarly, the European Court of Human Rights has held that surveillance must be accompanied by clear law and effective oversight to prevent abuse.

At the international level, human rights instruments recognise privacy as a core right. Article 17 of the *International Covenant on Civil and Political Rights* prohibits arbitrary or unlawful interference with privacy, requiring states to ensure that such interference is lawful, necessary, and subject to safeguards (UN Human Rights Committee, 2018).

These comparative standards offer important lessons for Indian constitutional jurisprudence. They highlight the need for precise surveillance laws, independent oversight mechanisms, and effective remedies. Incorporating these principles would strengthen India's privacy jurisprudence while balancing security with constitutional democracy.

IV. CHALLENGES IN REGULATING MASS SURVEILLANCE IN INDIA

Regulating mass surveillance in India presents serious constitutional and institutional challenges. While surveillance capabilities have expanded rapidly due to digitalisation, the legal and regulatory framework has not evolved at the same pace. This imbalance creates risks for fundamental rights, democratic accountability, and rule of law.

1. Absence of Comprehensive Data Protection Legislation

- i. India lacks a long-standing, comprehensive data protection framework that clearly governs the collection, use, sharing, and retention of personal data.
- ii. In the absence of a strong statutory regime, surveillance practices operate within fragmented sectoral laws that do not adequately define limits on state access to personal information.
- iii. The Supreme Court has emphasised that informational privacy requires legislative protection, especially in data-driven governance systems (Supreme Court of India, 2017).
- iv. Without enforceable principles such as purpose limitation, data minimisation, and user consent, surveillance activities risk becoming excessive and constitutionally disproportionate.

2. Technological Opacity and Lack of Transparency

- i. Modern surveillance relies on complex digital technologies such as algorithmic monitoring, metadata analysis, and data aggregation across platforms.
- ii. These technologies often function as “black boxes,” making it difficult for citizens to understand how data is collected, analysed, or used for decision-making.
- iii. Lack of public disclosure regarding surveillance programs weakens transparency and prevents meaningful democratic debate (Lyon, 2018).
- iv. When surveillance systems operate secretly, individuals are unable to challenge misuse or even know when their rights have been affected, undermining procedural fairness.

3. Weak Institutional Oversight Mechanisms

- i. Oversight of surveillance in India is largely internal and executive-controlled, with limited involvement of independent or judicial bodies.

- ii. Authorisation, review, and continuation of surveillance measures are often handled by the same branch of government that conducts surveillance, raising concerns of conflict of interest (Bhandari, 2020).
- iii. Parliamentary scrutiny of surveillance frameworks remains minimal, and there is no dedicated independent regulator with powers to audit or investigate surveillance practices.
- iv. Weak oversight reduces accountability and increases the possibility of arbitrary or discriminatory monitoring, contrary to constitutional guarantees under Articles 14 and 21.

Need for a Rights-Based Surveillance Framework

The expansion of surveillance technologies in India has made it essential to move from a security-centric approach toward a **rights-based surveillance framework**. Such a framework recognises surveillance as an exceptional state power that must be carefully limited to protect constitutional values of liberty, dignity, and democracy. After the judicial recognition of privacy as a fundamental right, surveillance can no longer operate primarily through executive discretion; it must be structured around constitutional compliance and accountability.

i. Principles for Constitutional Compliance

A rights-based surveillance framework must be grounded in clear constitutional principles. Foremost among these is the requirement of legality, which demands that surveillance powers be authorised by precise and accessible laws enacted by Parliament. Vague or overly broad statutory provisions undermine predictability and invite arbitrary use. Second, surveillance must pursue a legitimate state aim, such as national security or the prevention of serious crime, and not merely the convenience of general governance. Third, the principle of necessity and proportionality requires that surveillance be strictly limited in scope, duration, and intensity, ensuring that the least intrusive means are adopted (Supreme Court of India, 2017). These principles collectively ensure that surveillance does not become routine or indiscriminate.

ii. Role of Parliament, Judiciary, and Independent Regulators

A robust rights-based framework depends on the effective functioning of multiple constitutional institutions. Parliament plays a central role by enacting comprehensive surveillance and data protection legislation that clearly defines powers, limits, and safeguards. Parliamentary debate and scrutiny are essential to ensure democratic legitimacy and transparency.

The judiciary functions as the guardian of fundamental rights. Courts must rigorously review surveillance measures to ensure compliance with constitutional standards and provide effective remedies in cases of abuse. Judicial oversight, particularly through prior authorisation or meaningful post-facto review, acts as a critical check on executive power (Bhandari, 2020).

In addition, independent regulators are necessary to bridge the gap between law and practice. An autonomous oversight body with investigative and auditing powers can monitor surveillance programs, ensure compliance with legal standards, and address citizen grievances. Independence from the executive is crucial for such regulators to function credibly.

iii. Strengthening Procedural and Substantive Safeguards

Procedural safeguards are crucial in preventing the misuse of surveillance powers. These include clear authorisation procedures, defined time limits, periodic review, and mandatory record-keeping. Transparency mechanisms, such as public reporting in aggregate form, can enhance accountability without compromising security interests.

Substantive safeguards focus on limiting the scope of what surveillance can achieve. Principles such as data minimisation, purpose limitation, and restricted data retention reduce the risk of profiling and misuse. Strong remedies for unlawful surveillance, including compensation and exclusion of illegally obtained evidence, further reinforce constitutional protections (Richards, 2013).

V. CONCLUSION

The growth of mass surveillance in India raises serious constitutional concerns relating to privacy, liberty, equality, and democratic accountability. Expansive surveillance powers, exercised largely through executive discretion and fragmented legal provisions, risk undermining the constitutional balance between state authority and individual rights. Judicial interventions have clarified that surveillance must comply with standards of legality, necessity, and proportionality, yet gaps in legislative clarity, institutional oversight, and transparency continue to persist.

Privacy must be reaffirmed as a core democratic value, not merely as an individual interest but as a structural safeguard that enables free expression, autonomy, and meaningful participation in public life. Without privacy, democratic citizenship is weakened, and constitutional guarantees become fragile.

The way forward lies in strengthening constitutional governance through comprehensive legislation, independent oversight mechanisms, and robust judicial review. Embedding surveillance within a rights-based framework will ensure that technological advancements serve public interest while preserving the foundational values of dignity, liberty, and the rule of law in the surveillance age.

REFERENCES

- [1] Bhatia, G. L. (2019). The transformative constitution: A radical biography in nine acts.
- [2] Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.
- [3] Richards, N. M. (1934). The Dangers of Surveillance” (2013) 126. *Harvard Law Review*, 7, 1934-at.
- [4] Ramanathan, U. (2010). A unique identity bill. *Economic and Political Weekly*, 10-14.
- [5] Bhandari, V., & Lahiri, K. (2020). The Surveillance State, Privacy, and Criminal Investigation in India: Possible Futures in a Post-PUTASWAMY World. *U. Oxford Hum. Rts. Hub J.*, 15.
- [6] Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Tech. LJ*, 31, 117.
- [7] Solove, D. J. (2010). *Understanding privacy*. Harvard University Press.
- [8] Sathe, S. P. (2002). Judicial activism in India. *Oxford University Press*.
- [9] Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. Macmillan+ORM.
- [10] *Joined Cases, C. (2014). 293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] para 47.*
- [11] *European Court of Human Rights. (2019). Big Brother Watch and Others v. United Kingdom.*
- [12] Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- [13] Supreme Court of India. (2015). *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- [14] Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. <https://indiankanoon.org/doc/91938676/>
- [15] Information Technology Act, 2000. Government of India. <https://www.meity.gov.in/content/information-technology-act-2000>
- [16] *People’s Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301. <https://indiankanoon.org/doc/1033166/>
- [17] United Nations Human Rights Committee. (2018). *General Comment No. 16 on Article 17 (Right to Privacy)*. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-16-article-17>